



Privacy notice for visitors attending the offices of Pension Insurance Corporation plc.

(updated 3 February 2022)

1. Introduction

This notice is for all visitors to Pension Insurance Corporation plc ("PIC") offices. For the purpose of this privacy notice, 'visitor' is deemed to mean any individual not provided with credentials allowing access to PIC's email, network or other IT systems with the exception of guest access to the internet via Wi-Fi.

- This privacy notice explains what we do with your personal information when you visit PIC's offices.
- It describes how we collect, use and process your personal information, and how we comply with our legal obligations to you when doing so. Your privacy is important to us, and we are committed to protecting your rights.
- For the purpose of the relevant data-protection legislation (including the General Data Protection Regulation the 'GDPR') and Data Protection Act 2018 ('DPA2018') we, Pension Insurance Corporation plc of 14 Cornhill, London, EC3V 3ND, are responsible for your personal information. You can contact our Data Protection Officer by emailing us at dataprotection@pensioncorporation.com.
- The GDPR came into effect on 25 May 2018 and became the UK GDPR on 31 January 2021, and any references we make to it include the UK Data Protection Act 2018.
- This privacy policy is not a contract and we may amend it from time to time. We will make any changes to the online version of the policy, so please check our website for updates.
- If you are not satisfied with any part of our privacy policy, you may have legal rights. We have described these below (where relevant).
- When you visit our website, we collect different kinds of personal information about you and we may use this information for different purposes to those set out in this privacy policy. For details on how we handle the personal information that we collect about you when you visit our website, please see our general privacy policy at <https://www.pensioncorporation.com/privacy-policy/>.

2. What kind of personal data does PIC collect if you visit our offices?

We need to collect and use information about you when you visit our offices. This information could include the following.

- Your name
- Photographic, or video, images of you

We need this personal information that we collect from you so that we can ensure the security of our offices and the safety of you and our staff members.

In the event that you experience medical difficulties or suffer an accident during your visit and we need to administer first aid, contact a relative in order for them to assist you, or to request medical assistance on your behalf, we may also collect the following information:

- Your contact address
- Your Age
- Your Sex
- Your next of kin

We would not ordinarily collect this information from you and would only do so in order to be able to inform medical practitioners of these details should you become unable to do so.



3. How do we collect your personal information?

We collect personal information from you when you visit our offices in the following ways:

Personal data you give to us

- When you notify us that you intend, or wish, to visit our offices;
- When you report an accident, or incident, which you experience or witness during your visit to our offices.

Personal data that we collect via electronic security controls

- Access Control System if you are issued with an electronic ID card;
- Closed Circuit Television (CCTV) system.

4. How do we use your personal information?

The main reason we use information about you is to make sure you and our staff remain safe and secure when you visit our offices.

To support this, we use the following processes and systems:

Visitors Register

We maintain a register of visitors which includes visitors, contractors and other persons who have not been provided with credentials that would permit access to our IT systems. For this register we will collect the following information:

- First and last name; we may also ask for the name of the company you represent.

This information is collected for health and safety and security purposes.

Accidents and Incident Reporting

In accordance with our legal duties, PIC maintains a record of accidents and incidents that arise out of work activities.

PIC will collect personal data from you if you are injured or become ill whilst in our offices; we will collect the following information:

- Name, Address, Age, next of kin, details of the incident to include any relevant medical history.

This data is collected because PIC has a legal duty to maintain a record of workplace incidents/accidents and to report certain types of accidents, injuries and dangerous occurrences arising out of its work activity to relevant authorities.

Incidents and accidents will be investigated to establish what lessons can be learned to prevent such incidents/accidents re-occurring including introduction of additional safeguards, procedures, information instruction and training, or any combination of these. Monitoring is undertaken but on an anonymised basis. The information is also retained in the event of any claims for damages.

Access Control System

If you are issued with an ID card, our security system will collect the following information:

- Your name, Company name (where applicable). These details may be linked to an identifier (Card ID) that is specific to the ID Card you are issued with;
- Times swiped in and out of the building and our working floors.

The collected data will be used for recording and controlling access into and within PIC's offices.



Closed Circuit Television (CCTV)

CCTV is installed at strategic locations to provide a safe and secure working environment in our offices as part of PIC's commitment to safety, security and crime prevention.

The CCTV system covers our reception area and the area of entry and exit points to our offices including via interconnecting stairways; cameras are installed at the entrances, placed and focused in a way that only people who want to access the offices, or secure areas within our offices, are filmed.

PIC's CCTV system will collect the following information:

- Images of you entering and leaving our offices.

The collected data will be used:

- to control access to our offices and ensure:
 - the security of, our offices;
 - the safety of PIC staff and visitors;
 - the security of property and information located or stored on our premises.
- To prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure offices and protected rooms, IT infrastructure, or operational information.
- To prevent, detect and investigate a theft of equipment or assets owned by PIC, visitors of staff or threats to the safety of personnel working at our offices (e.g. fire, physical assault).

The CCTV system is not used for any other purpose, such as to monitor the work of employees or their attendance. It is important to notice that the location and positioning of the video-cameras are such that they are not intended to cover the surrounding public space, or the space occupied by other tenants within 14 Cornhill, London, EC3V 3ND. The cameras are aimed to give a general overview of what is happening in certain places but not to recognise persons.

The system is not used as an investigative tool or to obtain evidence in internal investigations or disciplinary proceedings unless a security incident is involved. In exceptional circumstances, the data may be transferred to investigatory bodies in the framework of a formal disciplinary or criminal investigation.

PIC's Chief People Officer ("CPO") is responsible for the operation of our CCTV System; on a day to day basis questions about PIC's use of CCTV may be raised via PIC's Facilities Manager.

5. Who do you share my personal information with?

PIC will only disclose information from the access control system, CCTV or visitors register where it is required to detect or prevent crime. This is usually on receipt of a Police issued personal data request form, required under Part 3 of the UK Data Protection Act 2018. There may be instances such as prevention of threat to life or serious injuries, where personal information would be provided without a signed police form.

6. How do we protect your personal information?

We place great importance on protecting your information and have appropriate measures in place to prevent anyone having unauthorised access to it or misusing it.

We are committed to taking appropriate steps to protect your personal information from misuse, loss, or unauthorised access. We will take appropriate technical and organisational security measures (including encryption and disaster recovery plans) to make sure that your information is treated securely and in line with this privacy policy.

If you suspect your information has been misused or lost, or that someone unauthorised has had access to it, please let us know immediately. Please contact us first. We will investigate the matter and update you as soon as possible on the next steps.



7. How long will PIC keep your data?

We will not keep your personal information for longer than is necessary for the purposes for which we collect it, unless the law or another regulation says we should keep it (for example, because of a request by a tax authority or in connection with legal action).

8. How can you access, amend or take back the personal information that you have given to us?

One of the GDPR's main aims is to protect and explain people's rights to do with data privacy. Even if we already hold your personal information, you still have various rights in relation to it, which we have set out below.

To get in touch about these rights, please contact us. We will try to deal with your request as soon as possible and always within one month (depending on any extensions to this period we are entitled to by law). We may keep a record of your communications to help us deal with any issues which you raise.

The GDPR gives you the following rights.

The right to object

You have the right to object to us processing your personal information if we do so:

- because it is in our legitimate interests;
- to help us perform a task in the public interest or to meet a request from an official authority;
- to send you marketing materials; or
- for scientific, historical, research or statistical purposes.

If your objection is about us processing your personal information because we think it is necessary for our legitimate interests, we must stop processing it unless:

- We can show that we have convincing legitimate reasons for processing your information which override your interests; or
- We are processing your information for the purposes of establishing or exercising a legal claim or in defence of a legal claim.

The right to withdraw permission

If we have obtained your permission to process your personal information for certain activities, you may withdraw this permission at any time and we will stop the activity that you agreed to, unless there is an alternative legal basis to justify us continuing to process your information. If this applies to you, we will tell you.

Data subject access requests (DSARs)

You can ask us to confirm what information we hold about you at any time, and ask us to alter, update or delete it. We will try to delete your personal information permanently, but some of it may still exist in our systems, for example if it is waiting to be overwritten (have new information recorded over it) or it is in our electronic back-up. The back-up is held on our systems until it is replaced in line with an established schedule. We may ask you for more information about your request. If we give you access to the information we hold about you, we will not charge you for this unless there are clearly no grounds for your request or it is 'manifestly unfounded or excessive'; for example, if you made the same request every week. If you ask us for further copies of this information, we may refuse your request. If we refuse your request, we will always tell you the reasons for doing so.



The right to delete your information

You have the right to ask us to delete your personal information in certain circumstances. Normally, the information must meet one of the following criteria:

- The information is no longer necessary for the purpose for which we originally collected or processed it.
- You have withdrawn your permissions to us to processing your information, and there is no other valid reason for us to continue processing it.
- The information has been processed unlawfully (that is, in a way which does not keep to data protection laws).
- The information needs to be deleted so that we can keep to our obligations as a data controller under UK law.
- It is information that we are processing because we believe it is necessary for our legitimate interests, you object to this, and we are unable to demonstrate we have overriding legitimate reasons for continuing to process it.

Under data protection law, we can only refuse to carry out your request for one of the following reasons.

- To keep to our legal obligations.
- For archive, research or statistical purposes.
- To enforce or defend a legal claim.

If we receive a valid request to delete information, we will take all reasonably practical steps to do so. We will try to delete it permanently, but some of it may still exist within our systems, for example if it is waiting to be overwritten (have new information recorded over it) or is in our electronic back-up. The back-up is held on our systems until it is replaced in line with an established schedule.

The right to restrict processing

You have the right to ask us to restrict processing your personal information in certain circumstances. This means that we can only continue to store your information and will not be able to process it until:

- one of the circumstances listed below is dealt with;
- you give your permission; or
- we need to process the information further for either the establishment, exercise or defence of legal claims, to protect the rights of another person, or for reasons of important UK state public interest.

You can ask us to restrict how we process your personal information in the following circumstances.

- If you believe the information is not accurate. In this case, we will restrict our processing while we confirm the accuracy of the information.
- If you object to us processing your personal information for our legitimate interests. In these cases, you can ask us to restrict the information while we confirm our reasons for processing your information.
- If the way we are processing your information is unlawful, but you would prefer us to restrict processing it rather than delete it.
- If we have no further need to process your information but you need the information to establish, exercise, or defend legal claims.

If we have shared your personal information with anyone else, we will tell them about the restricted processing unless this is impossible or involves an unreasonable amount of effort. We will tell you before we lift any restriction on processing your personal information.

The right to correct your information

You have the right to ask us to correct any inaccurate or incomplete personal information that we hold about you, including by providing additional information which we will keep with your information. If we have shared this information with anyone, we will tell them we have corrected it, unless this is impossible or involves an unreasonable amount of effort. You may also ask us for details of the people we have shared the information with. If we think that it is reasonable for us not to carry out your request, we will explain our reasons for this decision.



The right to transfer information

You have the right to transfer your personal information between data controllers. This means that you can transfer the details we have about you to a third party. To allow you to do so, we will give you your information in a commonly used machine-readable format so that you can transfer it. Or, we may transfer the information for you direct. This right applies to:

- personal information that we process automatically (that is, without any human intervention);
- personal information provided by you; and
- personal information that we process with your permission or to keep to a contract.

The right to lodge a complaint with a supervisory authority

You also have the right to complain to the Information Commissioner's Office. You can contact them in the following ways

- Phone 0303 123 113
- Email casework@ico.org.uk
- Live chat on their website <https://ico.org.uk/global/contact-us/live-chat>
- By post: Information Commissioner's Office, Wycliff House, Water Lane, Wilmslow, Cheshire SK9 5AF

If you would like to use any of these rights, or withdraw your permission to us processing your personal information, please contact us so that we can assist with your request. We may keep a record of your communications to help us sort out any issues which you raise.

9. Who is responsible for processing your personal information?

We are responsible for processing your personal information. Our address is 14 Cornhill, London, EC3V 3ND. You can contact our Data Protection Officer by emailing us at dataprotection@pensioncorporation.com.

If you have any comments or suggestions about this privacy policy, please contact us. We take privacy seriously and will get back to you as soon as possible and within any timeframe we have to keep to by law.

10. How do we store and transfer your information internationally?

So that we can carry out the purposes described in this privacy policy (for more details, please see section 4 'How do we use your personal information?') we may transfer your personal information to:

- law enforcement agencies (for more details, see section 5 'Who do you share my personal information with?')

We want to make sure that we store your personal information securely. We will only transfer it outside of the UK if it meets data-protection legislation and can be transferred in a way that protects it adequately. This could be done, for example:

- by transferring it to a country where the UK Information Commissioner's Office has found that levels of data protection are adequate; or
- if you have agreed that it can be transferred.



11. Legal bases for us processing your information

There are a number of ways that we are lawfully able to process your personal information.

a. When it is necessary to comply with a legal obligation

Article 6(1)(c) of the GDPR explains that we can process your information if it 'is necessary for compliance with a legal obligation to which we are subject.'

b. When it is in our legitimate interests

Article 6(1)(f) of the GDPR explains that we can process your information if it 'is necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of [you] which require protection of personal data.'

We do not think that processing your information will negatively affect you in any way. However, you do have the right to object to us processing your personal information on this basis. We have set out in section 8 how you can do this.

The table below summarises PIC's legal basis for your person information relative to the contexts in which we collect and process it:

Area or context	Legal basis	Further information
Access Control	Legitimate interests	It is in PIC's legitimate interests to ensure that there is a safe environment for work, and for visitors accessing our facilities.
Visitors Register	Legitimate interests	It is in PIC's legitimate interests to ensure that there is a safe environment for work, and for visitors accessing our facilities.
Accidents and incidents reporting	Legal requirement	This is a requirement under our Health and Safety obligations.
CCTV	Legitimate interests	It is in PIC's legitimate interests to ensure that there is a safe environment for work, and for visitors accessing our facilities.